INCIDENT RESPONSE

Il primo link

https://tinyurl.com/linklosco1 porta a un'analisi interattiva su ANY.RUN di uno script PowerShell denominato "DNS_Changer.ps1". Questo script sospetto è progettato per modificare le impostazioni DNS del sistema, potenzialmente reindirizzando il traffico Internet a server controllati dall'attaccante. L'attività di tale script potrebbe causare problemi di connettività o reindirizzare gli utenti a siti di phishing o malware.

Il secondo link

https://tinyurl.com/linklosco2 porta a un'analisi interattiva su ANY.RUN di un file sospetto ospitato su Google Drive. Questo file potrebbe essere correlato a attività malevole, come l'installazione di malware o la raccolta di informazioni sensibili dagli utenti che lo scaricano e lo eseguono.

Report di Analisi

Segnalazione dei Problemi: Due utenti hanno segnalato problemi sui loro computer.

Analisi del Primo Link:

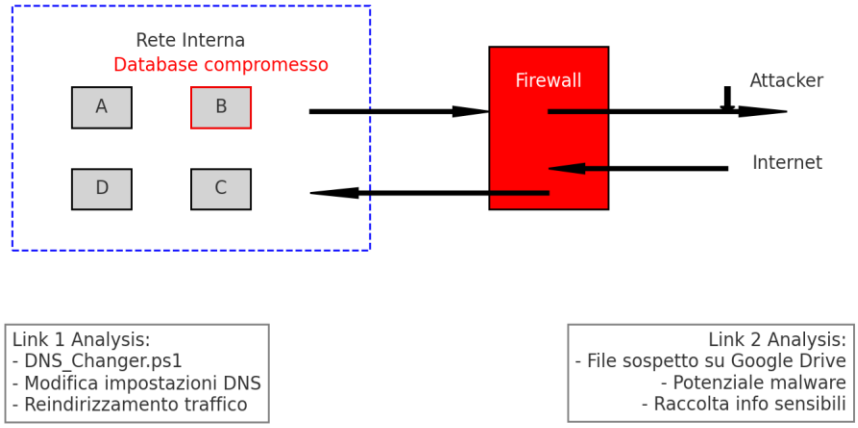
- **File:** DNS_Changer.ps1
- **Attività:** Modifica delle impostazioni DNS
- **Rischio:** Potenziale reindirizzamento del traffico a server malevoli.

Analisi del Secondo Link:

- **File:** Sospetto, ospitato su Google Drive
- **Attività:** Potenziale malware, raccolta di informazioni sensibili.

Conclusione:

- Gli utenti potrebbero essere vittime di un attacco mirato tramite script malevoli.
- Si consiglia una scansione completa dei sistemi interessati e un'analisi approfondita dei log di rete.



Ecco il grafico che rappresenta il contesto della rete e l'analisi dei due link sospetti segnalati dagli utenti.

Dettagli del Grafico:

1. **Rete Interna:**
   - Contiene i sistemi A, B (compromesso), C e D.
   - Il sistema B è evidenziato in rosso per indicare che è compromesso.
2. **Firewall:**
   - Situato tra la rete interna e Internet.
   - Blocca il traffico tra il sistema B e l'attaccante.
3. **Attacker e Internet:**
   - Mostrano la fonte dell'attacco e la connessione Internet.
4. **Analisi del Primo Link:**
   - **File:** DNS_Changer.ps1
   - **Attività:** Modifica impostazioni DNS
   - **Rischio:** Reindirizzamento traffico
5. **Analisi del Secondo Link:**
   - **File:** Sospetto su Google Drive
   - **Attività:** Potenziale malware
   - **Rischio:** Raccolta informazioni sensibili

Conclusione

- Gli utenti potrebbero essere vittime di un attacco tramite script malevoli e file sospetti.
- È necessario eseguire una scansione completa dei sistemi interessati e isolare temporaneamente i sistemi compromessi.
- Verificare le impostazioni DNS su tutti i dispositivi della rete e monitorare attentamente il traffico di rete per ulteriori attività sospette.